Integrating Mac OS X into a Heterogeneous Environment

Session 625

These are confidential sessions—please refrain from filming or taking pictures.

Enterprise IT

Integrating Mac OS X into a Heterogeneous Environment

Joel Rennich
Consulting Engineer
Enterprise Consulting Services

http://developer.apple.com/wwdc2005/

Introduction

- Using OS X with other Directory Services
- Using other operating systems with Open Directory

What You'll Learn

- How to integrate Tiger into other Directory Services
- How to integrate other operating systems into Open Directory
- How to setup file sharing in heterogeneous environments
- Possible backup solutions for heterogeneous environments

The OS X Island

Integrating OS X into other Directory Services

http://developer.apple.com/wwdc2005/

Plays Well With Others

- Directory Services
  - Users and groups
  - Passwords and Single Sign On
- File Sharing
- Backup

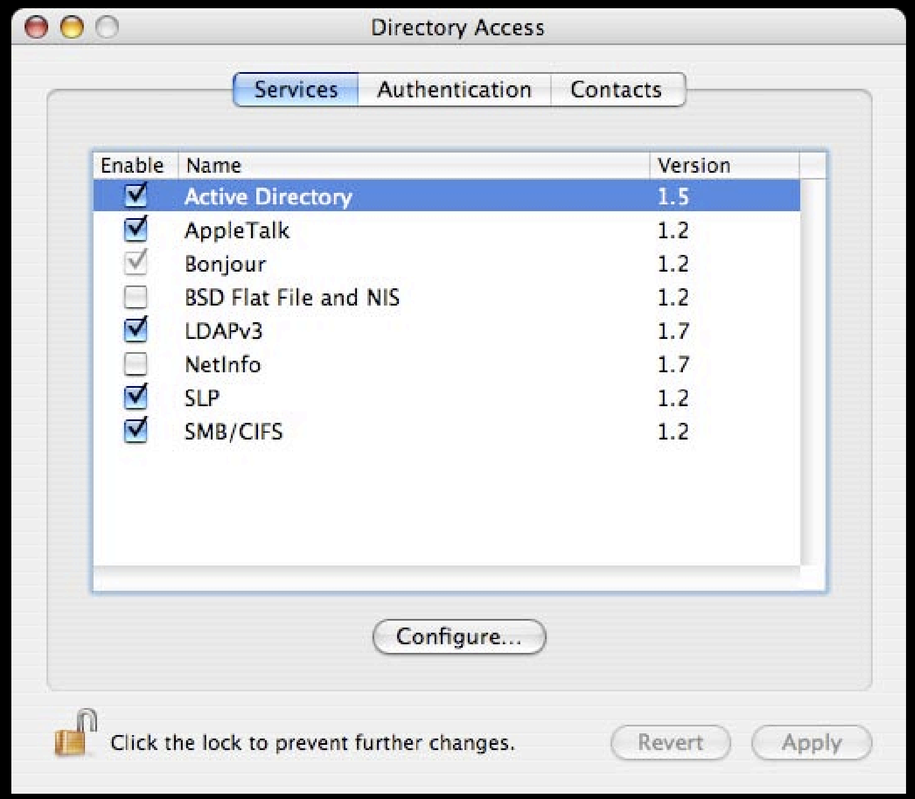
Directory Services

Identification and Authentication

http://developer.apple.com/wwdc2005/

Integration Options

- NIS
- Active Directory Plugin
- LDAP
- Third-Party Plugins
- Combination



NIS

- Only NIS not NIS+
- Holdover at best—not a long-term solution
- Migrate to other options

Active Directory

- AD Plugin
- Thursby ADmitMac
- Covered in other sessions

LDAP

- Closest to universal directory service solution
- Easily allows integration with many other directory services including SunOne, Novell, OpenLDAP, and sometimes Active Directory
- Best chance for interoperability

LDAP Integration Methods

- Use existing attributes
- Co-opt unused attributes
- Static assignment
- Variable mapping
- Extending the schema

Existing Data And Schema

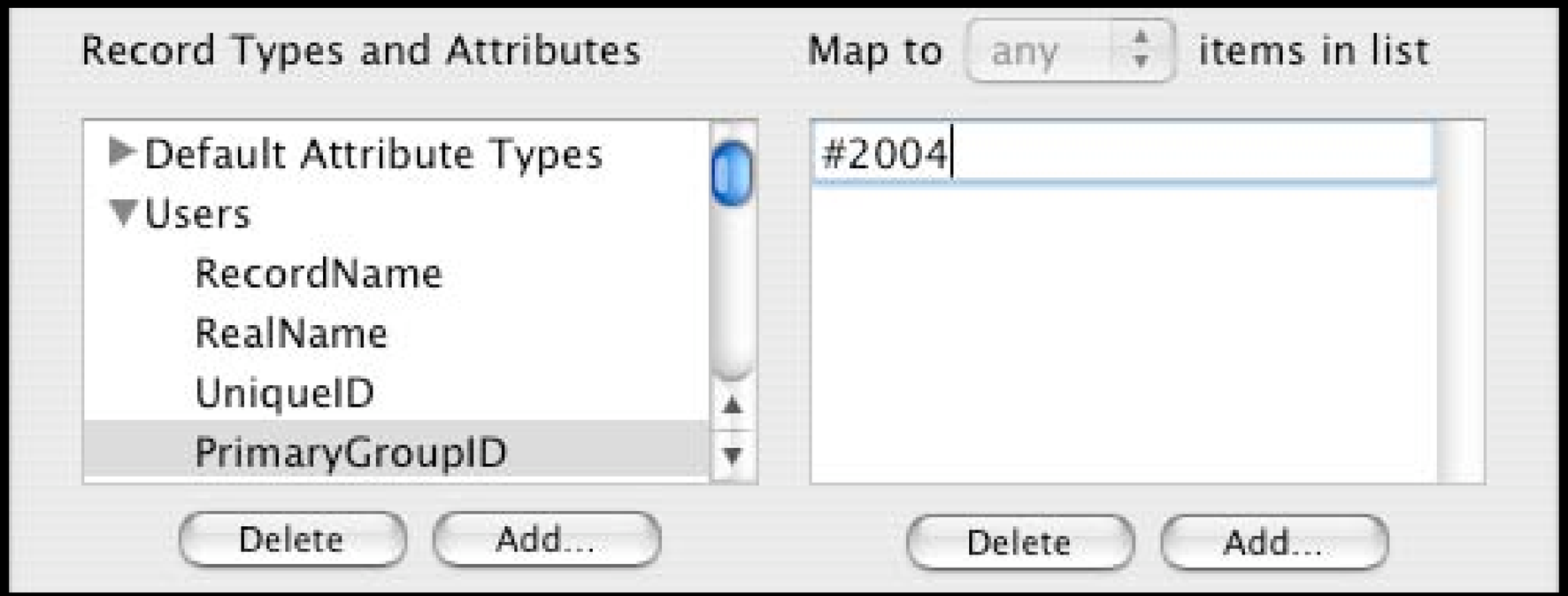
- Top priority is to use attributes and directory data as intended
- Existing user data should be reviewed
- Attributes with matching Mac OS X data requirements should be used and mapped in Directory Access
- User name, short name, password are present in most directories, but other values may also be available

Recycling Unused Attributes

- Unused attributes in a directory can be repurposed
  - The admin must carefully track and document the attributes being repurposed
  - Server updates and new services must be carefully tested before being deployed
  - Some risk for future conflict
- Minimal impact on directory structure and contents
  - Will need directory service admin's help

Static Assignment

- Mac OS X allows static assignments of attributes
- Instead of mapping to a field in LDAP, values can be assigned within the plugin's configuration
  - Type "#" and then the value



Variable Assignment

- Mac OS X allows static assignments to include other directory attributes
- Instead of mapping to a field in LDAP, values can be assigned within the plugin's configuration
  - Type "#" to enable the static and variable assignments
  - Nest the variable within $
  - Examples:
    - #/tmp/uid
    - #/Volumes/My_iPod/uid
    - #<home_dir><url>afp://server.apple.edu/Sharepoint</url><path>uid</path></home_dir>

Static And Variable Mappings Demo

http://developer.apple.com/wwdc2005/

Extend the LDAP Schema

- All directories allow for this, although some are less forgiving than others
- Can manually edit for simple changes
- Preferred method is to create and thoroughly test LDIF files to modify the schema
- Full schema extension provides one of the best Mac OS X user experiences
- Mac OS X client and server updates should be reviewed for new schema elements, or Apple's Knowledge Base should be consulted when updates are released

Novell

- Kanaka from Condrey Consulting
- Open Directory plugin for Novell
- Can also use LDAP

Instructions

http://www.condreyconsulting.com

Combining Directory Services

- OS X almost a Universal client
- Use any other Directory Service in addition to Open Directory
  - Users, most groups, and passwords in primary Directory Service
  - Management, groups, and machine lists in Open Directory
  - Can’t specify MCX for individual users
- Single point of user administration

Secondary Directory

- User attributes CANNOT be split across directories, but…
- Mounts, Groups, Printers, Computers Lists, and other classes of objects can be stored in a directory separate from Users (or each other)
- These attributes could be stored in
  - Local Netinfo domain
  - NetInfo parent domain on Mac OS X Server
  - LDAP directory on Mac OS X Server or other server

Enable	Configuration Name	Server Name or IP Address	LDAP Mappings	SSL
☑	Active Directory	192.168.0.5	Custom	☐
☑	OpenDirectory	192.168.0.10	Open Directory Server	☐

Directory Service Integration Options

Five basic levels

	Directory System	Flexibility	Management	Single Sign On
NIS	NIS	Minimal	None	No
Active Directory	Active Directory	Some	Minimal	Yes
LDAP	OpenLDAP, SunOne, others	Most	Full	Yes with Kerberos
3rd Party	Novell	Some	Some	No
Combination	**Any + Open Directory**	**Most**	**Almost Full**	**Maybe**

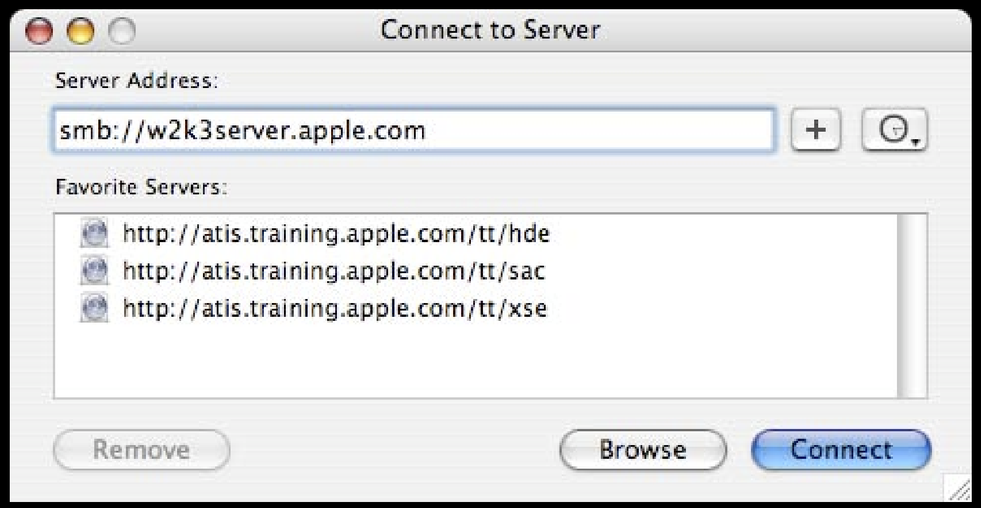
OS X Client to Linux Demo

http://developer.apple.com/wwdc2005/

File Sharing

Sea of protocols

http://developer.apple.com/wwdc2005/



File Sharing

- AFP
- SMB
- NFS
- FTP
- WebDAV

Apple Filing Protocol

- Preferred solution for OS X clients
- Most tested, most used
- Transparent fail over support
- AFP 3.1 Server
  - Novell NFA
  - Xinet Extreme Z-IP- NOT Services for Macintosh
  - Netatalk

Server Message Block

- Supported for home directories
- Windows Servers
  - Disable signing/encrypting
  - No DFS—use ADmitMac
- Samba Servers
- NAS devices

NFS

- Supported for home directories
- Much Improved in Tiger
- Kerberized in Tiger
- Supports Fast User Switching for network users
- Unix/Linux Servers
- NAS devices

FTP

- Not for home directories
- Read/only in the Finder

WebDAV

- Not for home directories
- Improved in Tiger
  - Kerberos authentication
  - SSL support
- Not good for complex permission schemes

Backup

http://developer.apple.com/wwdc2005/

Backup Clients on OS X

- BRU
- Retrospect
- Atempo
- Arkeia
- Tivoli
- Veritas
- Breece Hill
- Legato
- ARCserve
- BakBone

Open Directory for Other Systems

Integrating other operating systems into Open Directory

http://developer.apple.com/wwdc2005/

Plays Well With Others

- Directory Services
  - NT PDC for basic Windows support
  - LDAP for other sytems
- File Sharing
- Backup

Directory Services

http://developer.apple.com/wwdc2005/

NT PDC

- Support for PDC and BDC in Tiger
- Can use NT tools to manage PCs
- Good for limited setups
  - < 100 PCs
  - For larger installations go Cross-Realm

Open Directory LDAP

- Common Directory Service amongst non-Windows clients
- Easy integration with most Linux distributions and many Unix systems
- Group membership
  - Other systems won’t support new Tiger nested groups
  - We now list group members by full DN

Configuring Linux/Unix for OD

- /etc/nsswitch.conf—add “ldap”
- /etc/ldap.conf—add information about Open Directory Server
- /etc/pam.d/system-auth—add pam_ldap as an auth source
- /etc/fstab—add nfs mount of server home directories to replicate OS X network home directory mount path

Kerberos

- Single Sign On
  - Windows with Cross-Realm
  - Unix/Linux
- Standard MIT setup on OS X Server

Kerberos Configuration

- /etc/krb5.conf—copy from /Library/Preferences/edu.mit.kerberos
- kdamin -p admin@OD.EXAMPLE.COM—create service principles for host and other services
- Configure services to use keytab—may need to compile those services with Kerberos support

Linux to Open Directory Demo

http://developer.apple.com/wwdc2005/

Distributed Authorization in OD

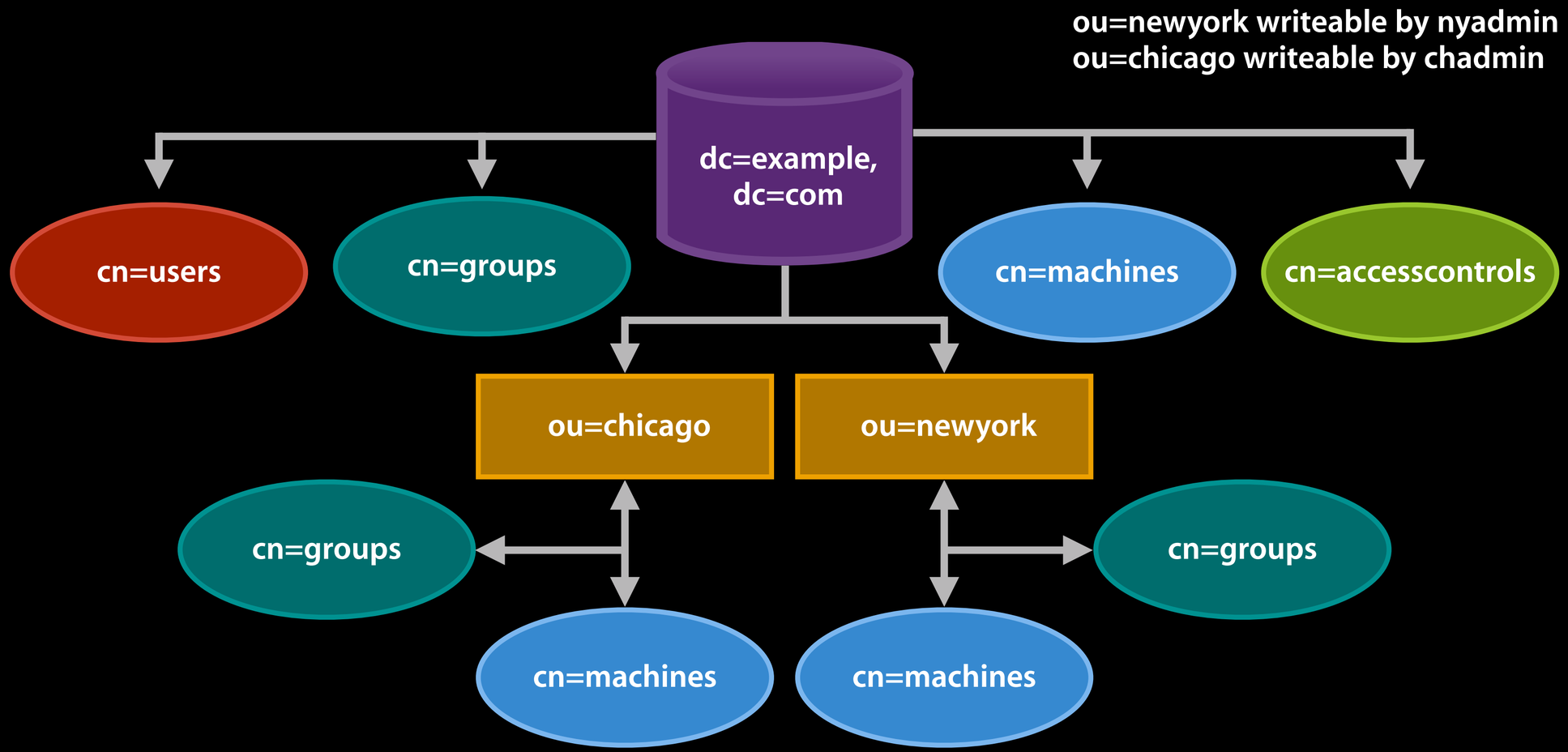
- What is it?
  - Delegate certain administrative tasks to non-admins
  - Permit use of Workgroup Manager
  - Make use of OU's
- How?
  - Essentially, a combination of custom mappings and ACL's

Distributed Authorization in OD

- Create OU's (phpldapadmin is a nice tool)
- Delegate administration using LDAP ACL's
  - Use WGM's All Records tab to add another value to the AccessControlEntry attribute on the default AccessControl entry
  - `1300:access to dn.sub=”ou=marketing,dc=example,dc=com” by group/posixGroup/memberUid="cn=admin,cn=groups,ou=marketing,dc=example,dc=com" write by * read`
- Custom mappings
- WGM unlocks if you can authenticate as a user in the “admin” group, even if it is not the domain-level admin group.

Map Machines and Groups to Particular OUs of Client Machines

- This allows for the subdivision of admins over machine lists and groups



File Sharing

http://developer.apple.com/wwdc2005/

AFP

- Probably won’t use for non-Apple clients
- Very little client support outside of OS X

SMB

- Samba 3.0.12
- Support for single sign on
- ACL support in Tiger

NFS

- Much improved in speed in Tiger
- Easy support for Unix/Linux clients

FTP

- Universal file sharing
- Basic options with built-in FTP server in OS X Server, but can use any one of a number of other FTP servers

Backup

http://developer.apple.com/wwdc2005/

Backup Servers on OS X

- BRU
- Retrospect
- Atempo
- Breece Hill
- BakBone

Q&A

http://developer.apple.com/wwdc2005/

More Information

http://developer.apple.com/wwdc2005/

Documentation, Sample Code, and Other Resources

http://developer.apple.com/wwdc2005/

WWDC2005

Worldwide Developers Conference